quire little processing power or computer memory. The only security precautions which are needed in accordance with the present invention are taken at the authentication center. The authentication center may be practiced, for example, in a conventional personal computer, and only one authentication center is required for the entire environment within which the present invention is practiced. The use of continually advancing sequence numbers in conjunction with authenticating with a public key algorithm provides strong security against pirating services without costly key management procedures. In place of costly secure key management procedures inexpensive nonvolatile memory technology is used to allow for "disposable" authentication codes. The sequence numbers provide security because the authentication codes are only used once. Memory technology provides a way to store enough authentication codes so that disposability is possible. The public key like algorithm allows for distribution of decryption keys to authentication nodes over non secure communication links. It also prevents the altering of "disposed" authentication codes to make them valid codes.

The present invention has been described above with reference to a preferred embodiment. However, those skilled in the art will recognize that changes and modifications may be made in this preferred embodiment without departing from the scope of the present invention. For example, those skilled in the art may devise a similar system which does not use user IDs but which encrypts each equipment ID with its own unique encryption key.

In addition, while the above described authentication system and method functions without a user PIN, use of a PIN is not precluded. For example, a PIN unique to each user may be assigned to or entered by the user and included in Log on message **116** in plain or encrypted form and verified in much the same manner as has already been described in connection with FIGS. **4–12**. However, such PIN number is not essential.

These and other changes and modifications which are obvious to those skilled in the art are intended to be included within the scope of the present invention.

What is claimed is:

1. A method for authenticating, by an authentication center having a first processor contained therein, user terminals used by users of a communication service offered by a communication service provider, said communication service being accessible through at least one user terminal of said user terminals, said one user terminal including a second processor contained therein, said user terminal having equipment identification data (ID) associated therewith and having pre-encrypted messages including sequence numbers stored therein, said method comprising steps of:

(a) obtaining by said first processor, said equipment ID for said one user terminal;

(b) obtaining by said first processor, said sequence numbers for said one user terminal;

(c) forming at said authentication center by said first processor, an encrypted block, said encrypted block including said equipment ID and said sequence numbers;

(d) storing said encrypted block in said one user terminal, said pre-encrypted messages comprising said encrypted block; and

(e) receiving a log-on message from said one user terminal to said communication service provider at least at initiation of a communication session, said log-on message including one of said pre-encrypted messages and said equipment ID.

2. A method as claimed in claim **1** wherein said step (c) comprises the steps of:

(c1) combining said equipment ID associated with said one user terminal with said sequence number to form a combined block, said sequence number being from a list of numbers in a particular order;

(c2) encrypting said combined block to form said encrypted block; and

(c3) repeating said steps (c1) and (c2) for each of said sequence numbers of said list of numbers to form a list of encrypted blocks which comprise said pre-encrypted messages, and said step (d) additionally comprises the step of storing said pre-encrypted messages in said one user terminal, and said step (e) additionally comprises the step of receiving a log-on message including one of said pre-encrypted messages stored in said one user terminal.

3. A method as claimed in claim **1** wherein said step (c) comprises a step of including first user identification data (ID) in said encrypted block.

4. A method as claimed in claim **1** wherein:

said step (c) includes a step of using a secret key in forming said encrypted block; and

said method additionally comprises a step of sending a public key to said communication service provider, said public key complementing said secret key.

5. A method as claimed in claim **1** wherein:

said step (c) includes a step of generating expiration date data for association with said encrypted block;

said step (d) includes a step of storing said expiration date data in said one user terminal; and

said log-on message includes said expiration date data with said pre-encrypted message and said equipment ID.

6. A method as claimed in claim **1** wherein:

said step (c) includes a step of programming an authentication module to store said encrypted block; and

said step (d) comprises a step of physically combining said authentication module with said one user terminal.

7. A method as claimed in claim **6** wherein said step (c) is performed at a location remote to said one user terminal, and said method additionally comprises a step of transporting said authentication module from said remote location to said one user terminal.

8. A method as claimed in claim **1** wherein said step (c) uses an encryption key to form said encrypted block, and said method additionally comprises steps of repeating said step (c) and said step (d) for said one user terminal from time-to-time, wherein different encryption keys are used during different repetitions of said step (c).

9. A method for authenticating user terminals used by users of a communication service accessible through said user terminals, wherein said user terminals-have pre-encrypted messages stored therein, said pre-encrypted messages including sequence numbers and equipment identification data (ID) associated with said user terminals, said method comprising steps of:

(a) receiving from one of said user terminals, a log-on message at initiation of each calling session, said log-on message including an encrypted block and an identifying block, said encrypted block being